RECEIVED
CENTRAL FAX CENTER

SEP 13 2007

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Previously Presented) A method comprising:

establishing a packet tunnel between a first local area network and a second local area network, the packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network;

reserving for the packet tunnel an amount of bandwidth within an access link;

detecting a network attack;

in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network;

establishing a first packet tunnel from the first local area network to the intermediate network device;

establishing a second packet tunnel that originates from the intermediate network device to the second local area network;

canceling the reserved bandwidth for the packet tunnel;

reserving for the second packet tunnel an amount of bandwidth within the access link; and

communicating virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first packet tunnel and forwarding the VPN traffic from the intermediate network device to the second local area network through the second packet tunnel.

2. (Original) The method of claim 1, wherein the source network address and the destination network address comprise port numbers.

3. (Original) The method of claim 1, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses.

4. (Previously Presented) The method of claim 1, wherein detecting a network attack comprises detecting an attack on the access link coupling a destination network device to a network.

5. (Canceled).

6. (Previously Presented) The method of claim 1, further comprising exchanging a set of available network addresses between a source network device originating the packet tunnel and a destination network device terminating the packet tunnel, wherein the set of available network addresses correspond to a plurality of intermediate network devices.

7. (Previously Presented) The method of claim 1, wherein splitting the packet tunnel by selecting an intermediate device comprises:

maintaining a set of available network addresses for a plurality of available intermediate network devices, wherein the network addresses are within network address spaces other than the address space of the first local area network and the address space of the second local area network; and

selecting one of the network addresses.

8. (Canceled).

9. (Previously Presented) The method of claim 1, further comprising:

upon detecting a network attack, sending a message from the destination network device to the source network device instructing the source network device to establish the first packet tunnel with the intermediate network device.

10. (Original) The method of claim 9, further comprising:

establishing a secure signaling channel between the source network device and the destination network device; and

sending the message via the secure signaling channel.

11. (Previously Presented) The method of claim 1, further comprising

de-encapsulating at the intermediate network device packets received from the first packet tunnel; and

re-encapsulating the packets at the intermediate network device for communication via the second packet tunnel.

12. (Previously Presented) The method of claim 1, further comprising:

establishing a secure signaling channel between a source network device and a destination network device;

sending via the secure signaling channel control packets between the source network device and the destination network device to monitor the performance of the first and second packet tunnels; and

selecting a new intermediate network device when the performance reaches a minimum threshold.

13. (Previously Presented) The method of claim 12, further comprising maintaining a set of possible intermediate network devices for a plurality of available intermediate network devices, wherein the network addresses are within network address spaces other than the address space of the first local area network and the address space of the second local area network, and wherein selecting the intermediate network device comprises selecting one of the possible intermediate network devices from the set.

14. (Previously Presented) The method of claim 1, wherein reserving an amount of bandwidth comprises sending a reservation message from a destination network device terminating the packet tunnel to a service provider access device.

15. (Original) The method of claim 14, wherein sending a reservation message comprises sending the reservation message according to the Resource Reservation Protocol (RSVP).

16. (Original) The method of claim 1, wherein establishing a packet tunnel comprises:

maintaining a set of available multicast network addresses;

selecting one of the multicast network addresses for the packet tunnel; and

subscribing to a multicast channel for the selected multicast network address.

17. (Previously Presented) The method of claim 16, wherein establishing a second packet tunnel comprises:

unsubscribing to the multicast channel;

selecting one of the multicast network addresses for the destination network address;

establishing the second packet tunnel using the new destination address; and

subscribing to a multicast channel for the selected multicast network address.

18. (Withdrawn) A method comprising:

establishing a packet tunnel having a source network address and a destination network address; and

establishing for the packet tunnel a truncated reservation path within an access link coupled to a destination network device that terminates the packet tunnel.

19. (Withdrawn) The method of claim 18, wherein the source network address and the destination network address comprise port numbers.

20. (Withdrawn) The method of claim 18, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses.

21. (Withdrawn) The method of claim 18, wherein establishing a truncated reservation path comprises issuing a reservation command from the destination device to reserve an amount of bandwidth within the access link for the packet tunnel.

22. (Withdrawn) The method of claim 18, further comprising:

detecting a network attack; and

canceling the truncated reservation path for the packet tunnel upon detecting the network attack.

23. (Withdrawn) The method of claim 22, further comprising:

establishing a new packet tunnel upon detecting the network attack; and.

reserving for the new packet tunnel an amount of bandwidth within the access link.

24. (Withdrawn) The method of claim 18, wherein establishing a truncated reservation path comprises sending a reservation message from a destination network device terminating the packet tunnel to a service provider access device coupled to the destination network device via an access link, wherein the reservation message indicates that packet flow for the tunnel terminates with the destination device.

25. (Withdrawn) The method of claim 24, wherein sending a reservation message comprises sending the reservation message according to the Resource Reservation Protocol (RSVP).

26. (Withdrawn) The method of claim 18, wherein detecting a network attack comprises detecting an attack on an access link coupling the destination network device to the network.

27. (Previously Presented) A method comprising:

establishing virtual private network service including a packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network;

reserving for the packet tunnel an amount of bandwidth within an access link;

detecting a network attack;

establishing new virtual private network service upon detecting the network attack by selecting an intermediate network device having a network address from a network address space other than the address space of the first local area network and the address space of the second local area network;

establishing a first packet tunnel from the first local area network to the intermediate network device; and

establishing a second packet tunnel that originates from the intermediate network device to the second local area network;

canceling the reserved bandwidth for the packet tunnel after establishing the new virtual private network service; and

reserving for the second packet tunnel an amount of bandwidth within the access link upon canceling the reserved bandwidth for the packet tunnel.

28. (Canceled).

29. (Original) The method of claim 27, wherein establishing a packet tunnel comprises:

maintaining a set of available multicast network addresses;

selecting one of the multicast network addresses for the destination network address of the packet tunnel; and

subscribing to a multicast channel for the selected multicast network address.

30. (Previously Presented) The method of claim 27, wherein detecting a network attack comprises detecting an attack on an access link coupling a destination network device to a network.

31. (Withdrawn) A method comprising:

maintaining a set of alternate multicast network addresses and a set of alternate unicast network addresses;

assigning one of the multicast network addresses to a packet tunnel terminating on a network device; and

assigning one of the unicast network addresses to a packet tunnel originating from the network device.

32. (Withdrawn) The method of claim 31, further comprising:

detecting a network attack; and

selecting a new multicast network address for the packet tunnel terminating on the network device upon detecting the network attack.

33. (Withdrawn) The method of claim 31, further comprising subscribing to a multicast channel for the multicast network address assigned to the packet tunnel terminating on the network device.

34. (Withdrawn) The method of claim 33, further comprising:

detecting a network attack;

unsubscribing to the multicast channel;

selecting a new multicast network address for the packet tunnel terminating on the network device upon detecting the network attack; and

subscribing to a new multicast channel for the new multicast network address.

35. (Previously Presented) A system comprising

a source device coupled to a first local area network; and

a destination device coupled to a second local area network,

wherein the source device and the destination device establish a packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network, reserve for the packet tunnel an amount of bandwidth within an access link, upon detecting a network attack, select a new network address from a network address space other than the address space of the first local area network and the address space of the second local area network, and split the packet tunnel by establishing a first packet tunnel from the first local area network to an intermediate network device having the network address and establishing a second packet tunnel from the intermediate network device to the second local area network,

wherein the destination device cancels the reserved bandwidth for the packet tunnel after the second packet tunnel is established, and reserves for the second packet tunnel an amount of bandwidth within the access link upon canceling the reserved bandwidth for the packet tunnel, and

wherein the source device communicates virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first packet tunnel for forwarding the intermediate network device to the second local area network through the second packet tunnel.

36. (Original) The system of claim 35, wherein the source network address and the destination network address comprise port numbers.

37. (Original) The system of claim 35, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses.

38. (Previously Presented) The system of claim 35, wherein the destination device and the source device comprise edge routers that couple local area networks to the network.

39. (Previously Presented) The system of claim 35, wherein the destination device detects an attack on an access link coupling the destination device to the network

40. (Canceled).

41. (Original) The system of claim 35, wherein the destination device and the source device exchange a set of available network addresses for the source network address and the destination network address of the packet tunnel.

42. (Original) The system of claim 35, wherein the destination device comprises a storage medium to store a set of available network addresses for use as the source network address and the destination network address of the packet tunnel.

43. (Canceled).

44. (Previously Presented) The system of claim 35, wherein the intermediate network device de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination device via the second packet tunnel.

45. (Previously Presented) The system of claim 35, wherein the source device and the destination device establish a secure signaling channel and send via the secure signaling channel control packets to monitor the performance of the first and second packet tunnels.

46. (Original) The system of claim 45, wherein the destination device selects a new intermediate network device when the performance reaches a minimum threshold.

47. (Withdrawn) A system comprising

a source device coupled to a network by a first access link, wherein the source device originates a packet tunnel; and

a destination device coupled to the network by a second access link, wherein the destination device terminates the packet tunnel, and further wherein the destination device establishes for the packet tunnel a truncated reservation path within the second access link.

48. (Withdrawn) The system of claim 47, wherein the destination device issues a reservation command to a service provider device to reserve an amount of bandwidth within the second access link.

49. (Withdrawn) The system of claim 47, wherein the destination device cancels the truncated reservation path upon detecting a network attack.

50. (Withdrawn) The system of claim 49, wherein the destination device establishes a new packet tunnel upon detecting the network attack and reserves for the new packet tunnel an amount of bandwidth within the second access link.

51. (Canceled).

52. (Canceled).

53. (Previously Presented) A computer-readable medium comprising instructions to cause a processor to:

establish a packet tunnel having a source network address within an address space of a first local area network and a destination network address within an address space of a second local area network;

reserve for the packet tunnel an amount of bandwidth within an access link;

detect a network attack;

in response to the detected network attack, split the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network;

communicate the network address to the source device for establishing a first packet tunnel from the first local area network to the intermediate network device;

establish a second packet tunnel that originates from the intermediate network device to the second local area network;

cancel the reserved bandwidth for the packet tunnel;

reserve for the second packet tunnel an amount of bandwidth within the access link; and

receive virtual private network (VPN) traffic that was redirected from the first local area network to the intermediate network device through the first packet tunnel and forwarded the VPN traffic from the intermediate network device to the second local area network through the second packet tunnel.

54. (Canceled).

55. (Previously Presented) The computer-readable medium of claim 53, further comprising instructions to cause the processor to select the intermediate network device by:

maintaining a set of available network addresses; and

selecting one of the network addresses.

56. (Canceled).

57. (New) The method of claim 1, wherein the first local area network and the second local area network are separated by a public network, and wherein the intermediate network device has a network address from a network address space of the public network.

58. (New) The method of claim 27, wherein the first local area network and the second local area network are separated by a public network, and wherein the intermediate network device has a network address from a network address space of the public network.

59. (New) The system of claim 35, wherein the first local area network and the second local area network are separated by a public network, and wherein the intermediate network device has a network address from a network address space of the public network.

60. (New) The computer-readable medium of claim 53, wherein the first local area network and the second local area network are separated by a public network, and wherein the intermediate network device has a network address from a network address space of the public network.